Abstract

A recorder is composed of a drive 102 and a host 103 that mutually authenticate each other. A C2_G 141 of the drive 102 calculates a medium ID and a medium key and obtains a medium unique key. The medium unique key is encrypted using a session key Ks generated by the mutual authentication and transferred to the host 103. A title key generated by a random number generator 143 of the drive 102 is transferred to the host 103. A content key calculated by a C2_G 145 of the drive 102 using the title key and the CCI 232 is encrypted using the session key Ks and then transferred to the host 103. A content is encrypted using a content key decrypted by the host 103. The drive 102 records the encrypted content, the encrypted title key, and the CCI 232 to the medium 101.